Atty. Docket No.: 042390.P8084
Express Mail No.: EL466333680US

APPLICATION FOR UNITED STATES PATENT

FOR

A DEVICE AND METHOD FOR DISABLING AN OVERRIDE HARDWARE PIN ASSERTION

Inventor(s):

DAVID W. GRAWROCK

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(714) 557-3800

BACKGROUND

1. Field

This invention relates to the field of data security. In particular, the invention relates to an apparatus and method for protecting confidential information stored within an electronic system.

2. Background

Advances in technology have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (e-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while electronic systems like computers provide users convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable for unscrupulous attacks. Examples of these attacks include virus, intrusion, exposure of private information, and tampering, to name a few. Therefore, it is becoming more and more important to protect the integrity of the contents of a computer, primarily to maintain user confidence in computer based transactions.

Recently, some Intel® Architecture computers are being employed with a firmware hub. To reduce the risk of unauthorized tampering with the stored contents of the firmware hub, control application software can be installed within the computer. The control application software is designed to preclude the deletion of data stored within flash memory of the firmware hub unless this software detects that the user correctly entered a previously negotiated pass phrase.

In the event that the pass phrase is forgotten by the user, the firmware hub includes an override pin which, when asserted, signals the control application software to

ignore the current pass phrase and enable a new pass phrase to be created. In certain situations, however, the override pin can be misused. For example, security features of a stolen computer can be deleted from the flash memory of the firmware hub after assertion of the override pin and entering of a new pass phrase selected by the thief.

There exists a need to temporarily disable the override pin to provide users of electronic systems with an ability to eliminate this recognized breach of system security.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an exemplary block diagram of an embodiment of a product employing an electronic system practicing the invention.

Figure 2 is an exemplary block diagram of an embodiment of the electronic system including a packaged IC device having an override disabled pin.

Figure 3 is an exemplary block diagram of the IC device of Figure 2.

Figure 4 is an exemplary block diagram of the pin configuration of the package of the IC device.

Figure 5 is an exemplary flowchart of the operations of the packaged IC device.

DESCRIPTION

The present invention relates to an apparatus and method for protecting information stored within an electronic system. More specifically, the invention comprises the addition of an override disable pin to the packaging architecture of an integrated circuit device such as the firmware hub for example. When asserted, the override disable pin sets a non-volatile bit storage element within the integrated circuit device. In the event that the override pin of the integrated circuit device is asserted, control application software running on the electronic system checks whether the non-volatile bit storage element is set and if so, denies the user access to information stored within the integrated circuit device unless a previously negotiated pass phrase is entered.

Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, terminology is used to discuss certain features of the present invention. For example, an "electronic system" includes any product that requires user authentication before providing access to its stored content. Examples of an electronic system include, but are not limited or restricted to a computer (e.g., desktop, a laptop, a server, a workstation, a hand-held, etc.), desktop office equipment (e.g., photocopier, printer, scanner, etc.), a television set-top box, and the like. A "link" is broadly defined as one or more information-carrying mediums (e.g., electrical wire, optical fiber, cable, bus, etc.) or wireless communications through infrared, radio frequency (RF) signaling, or any other wireless signaling mechanism.

In addition, the term "information" is defined as one or more bits of data, address, and/or control. A "pass-phrase" is a series of bits originating from a string of inputted alphanumeric characters, voice patterns and the like. In the context of information, the term "modify" (and related tenses) involves an act of either (i) adding, or (ii) deleting, or (iii) overwriting information. A "cryptographic operation" is an operation performed for additional data security such encryption, decryption, performing computations involving a digital signature, performing computations involving a digital certificate, and the like.

Referring to Figure 1, a perspective view of an illustrative embodiment of a product employing the present invention is shown. The product 100 comprises an electronic system 110 for processing data and a monitor 120 for displaying such data. The monitor 120 may include a flat panel display (e.g., liquid crystal display, active matrix display, etc.), a cathode ray tube, or any other type of display technology. The electronic system 110 further includes a receiver 130 to receive information over a link 140 and/or a transmitter 135 to transmit information over the link 140. For example, the receiver/transmitter 130/135 may include a modem that is situated external to a chassis 150 of the product 100 (as shown) or internal circuitry (e.g., a modem card, networking card, etc.) placed within the chassis 150.

Referring still to Figure 1, for this embodiment, the electronic system 110 receives as input information from one or more user input devices 160. The user input device 160 may be integrated within or physically remote from the chassis 150. Examples of a user input device 160 include, but are not restricted or limited to a keyboard, a keypad, a trackball, a mouse, a stylus, a microphone and the like.

Referring now to Figure 2, an illustrative block diagram of an embodiment of an electronic system 110 is shown. Electronic system 110 includes a processor 200, a memory control hub (MCH) 210, a system memory 220, an input/output control hub (ICH) 230, and a packaged integrated circuit (IC) device 240 (e.g., a firmware hub) which

supports communications with at least one of the user input devices 160 of Figure 1. The packaged IC device 240 features protected non-volatile memory memory and cryptographic logic as described in Figure 3.

In general, the packaged IC device 240 operates in a plurality of modes. For example, the packaged IC device 240 may be placed in an administrator mode when the user issues a request to alter the functionality of the electronic system 110. This is accomplished by controlling access to entering the administrator mode, possible through modification of its stored contents. Otherwise, the packaged IC device 240 operates in a user mode. For example, when performing cryptographic operation, like digitally signing information or encrypting/decrypting information, for example, the IC device 240 is in user mode.

As shown in Figure 2, the processor 200 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or hybrid architecture. In one embodiment, the processor 200 is compatible with the Intel® Architecture (IA) processor, such as the IA-32 and the IA-64. Of course, in an alternative embodiment, the processor 200 may include multiple processing units coupled together over a common host bus 205.

Coupled to the processor 200 via the host bus 205, the MCH 210 may be integrated into a chipset that provides control and configuration of memory and input/output devices such as the system memory 220 and the ICH 230. The system memory 220 stores system code and data. The system memory 220 is typically implemented with dynamic random access memory (DRAM) or static random access memory (SRAM). It is contemplated, however, that the system memory 220 may be segmented into an accessible physical memory area 221 and an isolated memory area 222. Access to contents within the isolated memory area 222 is restricted and enforced

by the processor 200 and/or the MCH 210 or other chipset that integrates the isolated area functionalities. The system memory 220 may also include other programs or data that are not shown.

The ICH 230 may also be integrated into a chipset together or separate from the MCH 210 to perform I/O functions. As shown, the ICH 230 enables communications to the packaged IC device 240 via link 250 from one or more user input devices 160 (e.g., a keyboard, keypad, etc.). Also, the ICH 230 enables communications to devices coupled to other links such as a Peripheral Component Interconnect (PCI) bus at any selected frequency (e.g., 66 megahertz "MHz", 100 MHz, etc.), an Industry Standard Architecture (ISA) bus, a Universal Serial Bus or another bus configured with a different architecture than those briefly mentioned.

Referring to Figure 3, an illustrative block diagram of the packaged IC device 240 is shown. The packaged IC device 240 comprises one or more integrated circuits placed within a protective IC package 300. For clarity sake, the packaged IC device 240 is based on an integrated circuit that comprises (i) logic 310 to perform a cryptographic operation, (ii) a non-volatile memory 315 (e.g., flash memory), and (iii) one or more control storage elements 330.

In particular, one portion of the non-volatile memory 315 is loaded with a representation 316 of the primary pass-phrase such as a hash value (result after the pass-phrase undergoes a one-way hash function) or any other computed value. Of course, the representation 316 could be the primary pass-phrase in its entirety.

Another portion of the non-volatile memory 315 includes microcode 317 that communicates with control application software executed by the processor 200 and accessible by the user. When the user desires to modify stored contents of the non-volatile memory, the control application software sends a message to the microcode 317

to determine whether or not access is granted or denied. One parameter of the message includes a previously negotiated, primary pass-phrase; however, other parameters of the message are based on the chosen Application Programming Interface (API) 318 between the microcode 317 and the control application software.

Another portion 319 of the non-volatile memory 315 is segregated into a plurality "N" of protected storage areas 320_1-320_N ($N \geq 1$), each having a predetermined size (referred to as "slots"). Each slot 320_1-320_N features an access control mechanism (ACM) 325_1-325_N that determines whether the user has access to the particular slot 320_1,..., 320_N. For example, access control mechanism 325_1 determines whether a secondary pass-phrase, provided by the user, indicates that user has access to the contents of the slot 320_1.

As further shown in Figure 3, the control storage element(s) 330 of the packaged IC device 240 is set upon assertion of an override disable pin 350. In one embodiment, the control storage element 330 includes one or more control registers configured for permanent state retention, namely maintaining its bit state through any number of power cycles. The control storage element 330 can be cleared only by providing the correct primary pass-phrase to place the packaged IC device into an administrator mode and clearing the state of the storage element 330 thereafter.

As shown in Figure 4, package 300 may include a 32-pin package featuring an override pin 340 and an override disable (OD) pin 350, although any size package may be used provided its pin configuration supports override and override disable signaling. In general, the assertion of the override pin 340 signals the control application software 225 to ignore the current, primary pass-phrase and allows the user to modify the primary pass-phrase. The assertion of the override disable pin 350 effectively signals the control application software running on the electronic system 110 to ignore the assertion of the

override pin 310 and still requires entry of the correct primary pass-phrase to gain access to stored content of the integrated circuit(s).

Referring now to Figure 5, a flowchart of the operations for disabling an override hardware pin assertion for the electronic system is shown. First, the user places the IC device into an administrator mode. For example, this may accomplished by the user selecting a control panel, which causes a window to be generated. The user enters a primary pass-phrase within a selected field of the window and selects an ENTER button on the window. The primary pass-phrase undergoes a computation (e.g., a one-way hash function) to produce a representation (e.g., hash value) and one or more parameters, inclusive of the representation, is transferred through the API to the microcode (blocks 500 and 510). The microcode compares the incoming representation with a prestored representation such as comparing the incoming hash value with a prestored hash value (block 520). If the primary pass-phrase is correct, the IC device is placed in the administrator mode (block 530). Otherwise, the IC device remains in its user mode.

During the administrator mode, the primary pass-phrase may be modified, the contents of the control storage element may be modified, or the contents of the slots within the non-volatile memory of the IC device may be deleted. However, if it is desirable to modify the contents of the first slot for example, the user is required to enter a secondary pass-phrase. Similarly, as described above, the input secondary pass-phrase undergoes a hash function to produce a hash value that is compared with a hash value prestored by the microcode. This prestored hash value associated with the first slot is contained in the storage area associated with the access control mechanism of the first slot. If the secondary pass-phrase is correct, the contents may be altered. Otherwise, the contents are not modifiable, but can be deleted and restored.

If the user fails to remember his or her primary pass-phrase, the override pin of the IC device may be asserted (block 540). If the override disable pin has not been

previously asserted so that the control storage element is set, the user may reconfigure the electronic system with a new primary pass-phrase (blocks 550 and 560). Upon selection, a representation (e.g., hash value) of the new primary pass-phrase is loaded into the non-volatile memory of the IC device (block 570). However, if the control storage element is set, the IC device signals the control application software that the user may not gain access to the stored content of the IC device unless the correct primary pass-phrase is entered (blocks 550 and 580).

In summary, in the normal case, when the override disable pin is not set, a system of the override pin allows the user to reset the primary pass-phrase and give access to the administrator mode. However, when the override disable pin is set, access to the administrator mode is restricted to only those parties who recall the primary pass-phrase.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.